Title of the Invention

METHOD AND SYSTEM FOR PROVIDING PERIMETER SECURITY

Technical Field of the Invention

This invention pertains to a method and a related system for providing perimeter security, as at a firefighting site, at a military site, at a transportation site, such as an airport or a train station, at a theme park, in an office building, or elsewhere. This invention contemplated that unique data displayed or recorded by a token, such as a card, a badge, or a ticket, which is presented by a person seeking entry, are read electronically, that the read data are compared to a database, via a computer having a display, and that a photographic image entered on the database of the person identified by the read data is displayed, via the display.

Background of the Invention

Since terrorist attacks in the United States on September 11, 2001, perimeter security has become a heightened concern at firefighting sites, particularly at firefighting sites where numerous firefighters are called upon, all of whom may not be personally acquainted with one another. Additionally, perimeter security has become a heightened concern at transportation sites, such as airports and train stations, at stadium events, at theme parks, in office buildings, and elsewhere. Historically, perimeter security has been a paramount concern at military sites, particularly at military sites where numerous military personnel are gathered.

Commonly, perimeter security has been addressed by issuing to each person authorized to enter a token, such as a card, a badge, or a ticket, which displays or records a unique set of data identifying said person, who can present the token when seeking to enter. The data are read by a human guard, if the data can be visually read, or by an electronic reader, if the data can be electronically read.

With printed cards, printed tickets, and other simple tokens, the data are susceptible to tampering or counterfeiting. As exemplified in numerous patents including United States Patents No. 5,214,699, No. 5,259,025, and No. 5,268,993, more complex tokens having electronic circuits to thwart tampering with the data on such tokens have been developed.

Summary of the Invention

This invention provides a method and a related system for providing perimeter security so as to restrict entry to authorized persons, who may be among a larger group of persons, not all of whom may be authorized. A token is issued to each authorized person or to each person of the larger group. The token displays or identifies a unique set of electronically readable data identifying that person, who can present the token when seeking entry. Moreover, a photographic image of each person of the larger population is entered into a database, which is maintained in a computer having a display, preferably a portable or hand-held computer. The data displayed or recorded by each token presented by a person seeking entry are read, via an electronic reader, and the read data are sent to the computer. The sent data are compared to the database, via the computer, and the photographic image entered on the database of the person identified by the sent data is displayed, via the display.

Brief Description of the Drawing

The drawing, which comprises a single figure, is a flow chart illustrating a preferred mode for carrying out this invention.

Detailed Description of the Preferred Mode

Broadly, a method and a related system are provided for providing perimeter security so as to restrict entry to authorized persons. If all persons of a group are

authorized, a token is issued to each person of the group. If the authorized persons are from a larger group of persons, not all of whom may be authorized, such a token is issued to each person of the larger group. In either instance, the token displays or records a unique set of electronically readable data identifying the person to whom the token has been issued, and who can present the token when seeking entry.

The token may be a card, a badge, a ticket or any other similar or dissimilar token. The token may display alphanumeric data, bar code data, a photographic image, and other similar and dissimilar data, which can be visually read. The token may record electronically readable data, as on an embedded chip or on a magnetic strip, which cannot be visually read.

A photograph image of each authorized person is entered into a database, which is maintained in a computer having a display, via data entry means. The data displayed or recorded by each token presented by a person seeking entry are read, via an electronic reader, are sent to the computer. The computer is programmed to compare the sent data to the database and to display, via the display, the photographic image entered on the database of the person identified by the sent data. Thus, a human guard can compare the appearance of the person presenting the token to the photographic image that is displayed, before deciding whether to allow the person resenting the token to enter.

In the preferred mode for carrying out this invention, the token is an identification card, the electronically readable data are bar code data, the electronic reader is a bar code reader, which is connected operatively to the computer, and the data entry means is a digital camera, which is connected

operatively to the computer. The bar code reader and the digital camera may be operatively connected to the computer via wired or wireless connections.

If the database is replicated on numerous computers, such as hand-held or portable computers carried by different personnel, it is difficult to an unauthorized person seeking entry to defeat the system, even if the unauthorized person is able to compromise the database maintained on some computers and to present a counterfeit, facially credible token, as the unauthorized person risks being detected via the database maintained on another computer. In a suspicious case, the data displayed or recorded on the token presented by a person seeking entry may be compared to the database maintained on each of plural computers.